

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER: _____**

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **07245605 A**(43) Date of publication of application: **19.09.95**

(51) Int. Cl. **H04L 9/00**
H04L 9/10
H04L 9/12
G09C 1/00

(21) Application number: **06033647**(22) Date of filing: **03.03.94**(71) Applicant: **FUJITSU LTD**

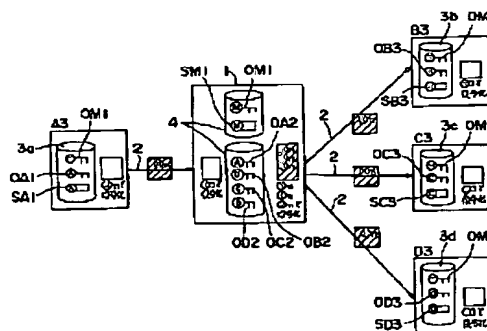
(72) Inventor: **KURODA YASUTSUGU**
KIKUCHI HIROAKI

**(54) CIPHERING INFORMATION REPEATER,
 SUBSCRIBER TERMINAL EQUIPMENT
 CONNECTING THERETO AND CIPHERING
 COMMUNICATION METHOD**

(57) Abstract:

PURPOSE: To minimize secret information to be managed by each member and to allow the method to flexibly cope with subscription / withdrawal of a member by allowing the ciphering information repeater to act like a management center of a secret key.

CONSTITUTION: A subscriber caller terminal equipment A3 ciphers information by using an open key OM 1 and sends the ciphered information to a communication line 2, a ciphering information repeater 1 receives the information and decodes the information into a plain text with a secret key SM 1. Then the repeater 1 ciphers again the plain text information with an open key OB 2 of a subscriber terminal equipment B and sends the ciphered information to the line 2. A terminal equipment B3 receives the information and decodes the information into a plain text with its own secret key SB 3. In the case of re-ciphering by the repeater 1, the repeater 1 uses open keys OC2, OD2 similarly to cipher the information and sends the ciphered information to terminal equipments C3, D3, which respectively decode the information into a plain text by using their own respective secret keys SC3, SD4. The repeater 1 centralizingly manages the open key information of each subscriber in this way and each subscriber has only to combine the common open key OM1 with its own open key and secret key. Thus, a subscriber's subscription/withdrawal is implemented by having only to rewrite data of the repeater 1.



【特許請求の範囲】

【請求項1】 通信回線（201）で接続された複数の加入者間（202a, 202b, 202c, 202d・・・・）で情報の送受信を行うシステムにおいて、前記発信加入者（202a）からの受信した暗号化情報の復号化、または受信加入者に送信する情報の暗号化を行う暗号計算部（203）と、前記暗号化情報を復号化するための共通秘密鍵（204）と、各加入者に対応した暗号化を行うための各加入者毎の個別公開鍵（205a, 205b, 205c, 205d・・・・）とを格納した鍵格納部（206）とを有する暗号化情報中継装置。

【請求項2】 前記に加えて、発信端末から発信加入者固有の秘密鍵で電子署名された情報を受信したときに、当該署名を検証するメンバ判断部を備えていることを特徴とする請求項1記載の暗号化情報中継装置。

【請求項3】 前記に加えて、発信加入者から受信した情報に基づいて秘密性の程度を変更可能な同報方式判断部を備えていることを特徴とする請求項1記載の暗号化情報中継装置。

【請求項4】 前記請求項1に記載した暗号化情報中継装置に接続される加入者端末であって、自身が送信する情報を暗号化するための共通公開鍵と、自身が受信した情報を復号化するための個別秘密鍵とを格納した鍵格納部を有していることを特徴とする加入者端末装置。

【請求項5】 発信加入者から加入者共通の公開鍵で暗号化された情報を受信した場合に、この情報を加入者共通の秘密鍵で復号化した後、当該情報を各加入者毎の個別公開鍵で暗号化して対応する受信加入者に送信する暗号通信方法。

【請求項6】 前記情報は発信加入者の秘密鍵によって電子署名がなされていることを特徴とする請求項5記載の暗号通信方法。

【請求項7】 前記秘密鍵によって電子署名された暗号化情報を受信した場合に、自身が有する当該発信加入者の公開鍵で前記電子署名を検証し、当該加入者が正規の加入者であるか否かを判定することを特徴とする請求項5記載の暗号通信方法。

【請求項8】 前記判定結果を前記発信加入者からの情報に添付して受信加入者に送信することを特徴とする請求項7記載の暗号通信方法。

【請求項9】 各加入者毎の個別公開鍵で暗号化して対応する受信加入者に送信する際に、加入者共通の秘密鍵で電子署名することを特徴とする請求項5記載の暗号通信方法。

【請求項10】 前記発信加入者は情報を暗号化することなく発信加入者が保有する秘密鍵によって情報に電子署名を行い前記暗号化情報中継装置に送信し、これを受信した前記暗号化情報中継装置は自身が保有している当該発信加入者の公開鍵を用いて電子署名を検証した後、

加入者共通の秘密鍵で電子署名して各加入者に送信し、受信加入者はこの情報を受信した際に自身が保有している加入者共通の公開鍵で当該電子署名を検証することを特徴とする請求項5記載の暗号通信方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、計算機を相互に接続したネットワークにおいて、情報の同報通信時の際の機密保持に適用して有効な技術に関する。

10 【0002】

【従来の技術】 近年のネットワーク環境下では、情報交換・提供の手段として電子メールや電子掲示板等が多用され始めてきている。

【0003】 この種のネットワークでは開放的なアーキテクチャに基づいてシステムが構築されているため、いわゆる電子メールののぞき見や第三者への機密情報の漏洩等が常に問題となっていた。

【0004】 上記に加えて、オンラインショッピングやホームバンキング等のようにネットワーク利用を前提とした商用サービスが次々と実現していくなかで、予期しない第三者への機密情報の漏洩は犯罪を誘発する要因となりかねない。

【0005】 このような点に鑑みて、ネットワーク上でのセキュリティを高めるため、送り手はデータを暗号化してネットワーク上に送信し、受信側では受信した暗号化データを解読して基のデータ形式に戻すという、いわゆる暗号通信システムが種々研究されている。

【0006】 同報通信（単一の送り手から複数の受け手に情報を送信する方式）において用いられている暗号通信方式としては下記のものがある。

【共通鍵方式】 「共通鍵方式」は、メンバ（発信者および受信者）が共通の公開鍵（暗号化するための鍵）と秘密鍵（復号化するための鍵）とを共有する形態である。発信者は、このメンバ間で共通の公開鍵を用いて情報を暗号化して送信する。これを受け取った受信者は、メンバ共通の秘密鍵で暗号化情報を復号（平文化）してその情報を読みとる方式である。これを図9を用いてさらに説明する。

【0007】 同図は、情報100を送信側のメンバ（暗号装置A1）から、受信側の各メンバ（暗号装置B1, C1, D1）に対して同報通信する場合を説明している。送信側の暗号装置A1の記憶部104内には、メンバ共通の公開鍵O1と、秘密鍵S1とが用意されている。暗号装置A1は、まず情報100を前記公開鍵O1で暗号化して送信する。そして同報通信された暗号化情報101, 101, 101を受け取った受信者側の暗号装置B1, C1, D1は、それぞれの記憶部104a, 104b, 104c内に用意している秘密鍵S1, S1, S1を用いて当該暗号化情報101, 101, 101を復号化して平文（102, 102, 102）とす

る。ここで平文とは人間または機械で可読な情報を指す。

【個別鍵方式】「個別鍵方式」では、各メンバがメンバのリストと全てのメンバの公開鍵のリストを共有する形態である。

【0008】発信者は、情報を各メンバ（受信者）の公開鍵で暗号化して送信する。これを受け取った受信者は、自身の秘密鍵で暗号化情報を復号化してその情報を読みとる。

【0009】この個別鍵方式を図10を用いて説明する。同図に示すように、送信側の記憶部107aには自身が受け取った暗号化情報を復号化するための秘密鍵SAとともに、各メンバの公開鍵OA、OB、OC、ODが保持されている。同様に、受信側の暗号装置B2、C2、D2の記憶部（107b、107c、107d）内においても自身の秘密鍵（SB、SC、SD）とともに各メンバの公開鍵（OA～OD）がそれぞれ保持されている。

【0010】ここで、A2より情報105を各メンバ（B2、C2、D2）に送信する場合、まずメンバB2の公開鍵O2を用いて暗号化した情報（暗号化情報105b）を作成し、同様にメンバC2の公開鍵OCを用いて暗号化情報105cを作成し、メンバD2の公開鍵ODを用いて暗号化情報を105dを作成した後、それぞれのメンバB2、C2、D2に送信する。

【0011】これらの暗号化情報を受信した各メンバB2、C2、D2ではそれぞれの秘密鍵SB、SC、SDを用いて平文化する（106b、106c、106d）。

【0012】

【発明が解決しようとする課題】ところが、上記従来技術では下記のような問題があった。

【0013】〔共通鍵方式の問題点〕メンバ共通の秘密鍵（S1）を、メンバ全員で管理するため、第三者に秘密鍵を知得されてしまう可能性が高く秘密漏洩を生じやすい。また、悪意を有するメンバが意図的に秘密鍵を横流しする不法行為も否定できなかった。

【0014】また、メンバがこの同報通信システムから脱会するときには情報漏洩防止のために、新たに残存メンバ共通の秘密鍵を再作成して残存メンバに配布しななければならない、同報通信システムの加入者が増加してくるとその管理が煩雑になる恐れがあった。

【0015】さらに、公開鍵が公開されることにより、予期しない第三者がこの同報通信システムに情報を送信することができるようになり、特定者間の情報流通の閉鎖性が損なわれてしまう可能性があった。

【0016】〔個別鍵方式の問題点〕各メンバが全メンバのリストと公開鍵を管理しなければ、各メンバの暗号装置における記憶部の負担が増大する恐れがあった。

【0017】また、メンバが同報通信システムに加入・

脱退するときには残存メンバが各々保持している加入者・脱退者の公開鍵の情報を更新させなくてはならず、同報通信システムの加入者が増減した場合にはその管理・維持が非常に煩雑になる可能性があった。

【0018】さらに、上記において各メンバが遠隔地に分散している場合、更新情報の伝達に時間がかかり、残存メンバ間の情報に矛盾を生じ、システムの円滑な運用が困難になる可能性もあった。

【0019】本発明は、前記課題に鑑みてなされたものであり、各メンバが管理しなければならない秘密情報を最小限に抑制し、メンバの加入・脱退にも柔軟に対応できる同報暗号通信システムを提供するものである。

【0020】

【課題を解決するための手段】本発明の第1の手段は、図1に示すように、通信回線201で接続された複数の加入者間202a、202b、202c、202dで情報の送受信を行うシステムであって、前記発信加入者202aからの受信した暗号化情報の復号化、または受信加入者に送信する情報の暗号化を行う暗号計算部206と、前記復号化するための共通秘密鍵204と、各加入者に対応した暗号化を行うための各加入者毎の個別公開鍵205a、205b、205c、205dとを格納した鍵格納部206とを有する暗号化情報中継装置としたものである。

【0021】第2の手段は、前記に加えて、発信端末から発信加入者固有の秘密鍵で電子署名された情報を受信したときに、当該署名を検証するメンバ判断部を備えるようにしたものである。

【0022】第3の手段は、前記に加えて、発信加入者から受信した情報に基づいて秘密性の程度を変更可能な同報方式判断部を備えたものである。第4の手段は、前記暗号化情報中継装置に接続される加入者端末について、自身が送信する情報を暗号化するための共通公開鍵と、自身が受信した情報を復号化するための個別秘密鍵とを格納した鍵格納部を有するものである。

【0023】第5の手段は、発信加入者から加入者共通の公開鍵で暗号化された情報を受信した場合に、この情報を加入者共通の秘密鍵で復号化した後、当該情報を各加入者毎の個別公開鍵で暗号化して対応する受信加入者に送信するようにした。

【0024】第6の手段は、前記第5の手段において前記情報に対して発信加入者の秘密鍵によって電子署名するようにした。第7の手段は、前記第5の手段において、前記秘密鍵によって電子署名された暗号化情報を受信した場合に、自身が有する当該発信加入者の公開鍵によって電子署名を検証し、当該加入者が正規の加入者であるか否かを判定するようにした。

【0025】第8の手段は、前記第7の手段において、前記判定結果を前記発信加入者からの情報に添付して受信加入者に送信するようにした。第9の手段は、前記第

5の手段において、各加入者毎の個別公開鍵で暗号化して対応する受信加入者に送信する際に、加入者共通の秘密鍵で電子署名するようにした。

【0026】第10の手段は、前記第5の手段において、前記発信加入者は情報を暗号化することなく発信加入者が保有する秘密鍵によって情報に電子署名を行い前記暗号化情報中継装置に送信し、これを受信した前記暗号化情報中継装置は自身が保有している当該発信加入者の公開鍵を用いて当該電子署名を検証した後、加入者共通の秘密鍵で電子署名して各加入者に送信し、受信加入者はこの情報を受信した際に自身が保有している加入者共通の公開鍵で当該電子署名を検証する暗号通信方法である。

【0027】

【作用】前記第1の手段によれば、暗号化情報中継装置を介在させることにより、この暗号化情報中継装置が暗号鍵の管理センターとして機能することにより、各加入者が共通の秘密鍵を共有することなく、機密の漏洩防止を効果的に実現できる。また加入者の脱退や新規加入の場合には、この暗号化情報中継装置に集中されたデータベースを更新するのみで良いため、加入者が増加した場合にもこれらの管理が煩雑にはならない。

【0028】第2の手段によれば、情報の送信に際して、発信加入者に加入者自身しか知らない個別秘密鍵で電子署名させることにより、暗号化情報中継装置では当該情報が正規の加入者から送られてきたものか否かを判別することができる。そのため、正規加入者以外の送信者からの情報を特定することができる。

【0029】第3の手段によれば、同報方式判断部を備えることにより、暗号化情報中継装置から送信する情報の秘密性の度合いを変更できる。したがってネットワークの状態に応じて必要以上の秘密化処理を行うことなく常に最適な秘密処理を選択できる。

【0030】第4の手段によれば、加入者端末として自身が送信する情報を暗号化するための共通公開鍵と、自身が受信した情報を復号化するための個別秘密鍵のみを保持すればよいため、各加入者が必要以上の秘密情報を管理することがなく、機密性を高めることができる。

【0031】第5の手段によれば、前記第1の手段同様、各加入者の共有する秘密情報（共通秘密鍵など）を最小限にすることができるため、機密の漏洩を効果的に防止できるとともに、加入者の増加にも柔軟に対応できる。

【0032】第6および第7の手段によれば、電子署名により送信加入者の正規性の判定を容易に行うことができ、たとえば脱退した元加入者が正規加入者になりすまして残存加入者に秘密情報を送信することを容易にチェックできる。

【0033】第8の手段によれば、受信側加入者は前記暗号化情報中継装置による判定結果を情報とともに受け

取ることにより、判定結果を参照して自身が読む必要のある情報か否かを判断することが容易となる。

【0034】第9の手段によれば、前記暗号化情報中継装置が加入者共通の秘密鍵で電子署名して情報を送ることにより、第三者が中継装置になりすまして情報を送信することを防止でき、前記暗号化情報中継装置と受信加入者との間の通信機密性をさらに高めることができる。

【0035】第10の手段によれば、情報を暗号化しなくても電子署名の検証により発信加入者の正当性を検証できる。要するに本発明によれば、暗号化して情報中継を行うことにより第三者による情報の盗聴を防止することができ、また電子署名した情報を中継することにより第三者が正当な発信者になりすますことを検出・防止できる。

【0036】

【実施例1】図2は、本発明の実施例1のシステム構成を示している。本実施例では、暗号通信の手段として、PEM (Privacy Enhanced Mail) を用いる。PEMは、インターネット (Internet) における標準化文書rfc 1421-1242に規定されている暗号電子メールの標準形式であり、情報を秘密鍵暗号DESで暗号化し、その鍵を公開暗号RSA (後述する) を用いて暗号化し送信するものである。

【0037】同図において、暗号化情報中継装置1は、通信回線2によって加入者端末装置A3、B3、C3とそれぞれ接続されている。本実施例では説明の便宜上、加入者A3 (加入者端末A3) から3名の加入者B3、C3、D3 (加入者端末B3、C3、D3) に暗号化情報を同報通信する場合で説明するが実際の秘密情報通信ではさらに多くの加入者への同報通信が必要であることはいうまでもない。

【0038】各加入者端末装置A3、B3、C3、D3にはそれぞれ鍵格納部3a、3b、3c、3dが設けられており、この鍵格納部内には共通の公開鍵OM1と各個々の端末 (加入者) の公開鍵と秘密鍵の対 (OA1とSA1、OB3とSB3、OC3とSC3、OD3とSD3) が登録されている。

【0039】暗号化情報中継装置1の鍵格納部4内には、共通公開鍵OM1と共通の秘密鍵SM1および各加入者の公開鍵OA2、OB2、OC2、OD2が登録されている。

【0040】ここで、「公開鍵」とは情報を暗号化するためのものであり、「秘密鍵」は暗号化された情報を復号化するものである。このような公開鍵と秘密鍵を用いた暗号方式としては、RSA (R. L. Rivest, A. Shamir, L. Adleman) が知られている。このRSAについて簡単に説明する。RSAが使用する数論特性は「 n に対して互いに素である i を $\phi(n)$ 乗し、 $\text{mod } n$ を掛けると1になる」という点である。これは次の式で表される。

50 【0041】

【数1】 $i \phi^{\omega}(\text{mod } n) = 1$

eおよびdをモジエロ $\phi(n)$ の逆数であるランダムは整数と仮定する。これを式で表すと次式ようになる。

【0042】

【数2】 $ed = 1 \pmod{\phi(n)}$

オイラーの定理では、Mがnに対して互いに素であるとき、次の二つの関係が成り立つ。

【0043】

【数3】 $(M^e)^d = M \pmod{n}$

$(M^d)^e = M \pmod{n}$

これを暗号法に適用すると、Mがメッセージ（情報）の一部であるとき、次の関数でメッセージをコード化できる

【0044】

【数4】 $s = M^e \pmod{n}$

一方復号するときには次の関数となる。

【0045】

【数5】 $M = s^d \pmod{n}$

次に、オイラーのファイ関数 $\phi(pq)$ を計算する。nを2つの素数の積とすると、 $\phi(pq) = (p-1)(q-1) = \phi(n)$ という式が成り立つ。

【0046】次に、 $\phi(n)$ に対して互いに素である値eを選択する。このとき、 $\max(p+1, q+1) < e < \phi(n)$ の範囲にある値を選択するとよい。さらに $(ed) = 1 \pmod{\phi(n)}$ となるような値dを計算する。すなわち $\phi(n)$ を法としたeの逆数を求めるのである。dの値が小さすぎたときには $(\log_2 n)$ 未満、eおよびdの値を変える。

【0047】メッセージmを暗号化するにはmをnより小さい固定サイズの整数Mに分割する。次にメッセージの各部分について $(M^e) \pmod{n} = s$ の値（これが公開鍵となる）を求める（本実施例では暗号計算部6が行う）。これらの値が連結されて暗号化情報が生成される（連結処理は情報作成部7で行ってもよい）。

【0048】このメッセージ（暗号化情報）を復号化するには、メッセージをブロックに分割し各ブロックを $(s^d) \pmod{n} = M$ （これが秘密鍵となる）で復号する。各加入者端末装置A3の内部構成をさらに詳しく示したものが図3である。同図において、共通公開鍵AM1、個別公開鍵OA1および個別秘密鍵SA1が格納されている鍵格納部3aは暗号計算部6からアクセスされる。情報作成部7は文書を作成するエディタ等を備えている。また通信インターフェース8は通信回線2との通信手順を実行する。これらの暗号計算部6、情報作成部7および通信インターフェース8は制御部5により制御される。これらの各部は具体的にはコンピュータシステムを用いて実現されており、鍵格納部3aは磁気記録媒体上に生成され、暗号計算部6は所定のロジックを制御部のプロセッサが実行することで実現されている。

【0049】図4は、本実施例における暗号化情報中継

装置1の内部構成をさらに詳しく説明したものである。

同図に示すように、鍵格納部11には共通公開鍵OM1およびこれに対応する秘密鍵SM1、そして各加入者の公開鍵OA2、OB2・・・が格納されている。

【0050】この鍵格納部11は、インデックスとして機能するメンバ情報格納部14を有しており、このメンバ情報格納部14には加入者の情報これに対応づけられた加入者の公開鍵とが登録されている。当該暗号化情報通信システムの管理者は、制御部12を通じてこのメンバ情報格納部14を修正・削除・追加することにより鍵格納部11を更新することができる。

【0051】鍵格納部11は、暗号計算部6からアクセスされ秘密鍵および公開鍵が読み出されるようになっている。メンバ判断部13は、発信端末からの情報に付された電子署名を解析して当該発信者が正当な加入者であるか否かを検証する。

【0052】通信インターフェースは、通信回線2との通信手順を実行する。これらの暗号計算部6、メンバ判断部13および通信インターフェース8は制御部12により制御される。これらの各部は具体的にはコンピュータシステムを用いて実現されており、鍵格納部11およびメンバ情報格納部14は磁気記録媒体上に生成され、暗号計算部6は所定のロジックを制御部12のプロセッサが実行することでその機能が実現されている。

【0053】次に以上に説明した図2～図4に基づいて、加入者端末A3から情報を暗号化して暗号化情報中継装置1を経由して各端末B3、C3、D3に配信する場合について説明する。

【0054】加入者発信端末A3では、情報をまず共通の公開鍵OM1で暗号化して暗号化情報を生成し、通信回線2上に送信する。当該暗号化情報を受信した暗号化情報中継装置1では、秘密鍵SM1でこの暗号化情報を平文化（人間または機械が可読な情報形式にすること）する。

【0055】次に、暗号化情報中継装置1は、加入者端末B3の公開鍵OB2を用いて前記平文化された情報を再度暗号化する。このようにして再暗号化された情報は、通信回線2上に送信される。これを受信した受信加入者端末B3では、自身の秘密鍵SB3を用いて前記再暗号化情報を平文化する。

【0056】前記再暗号化の際に、暗号化情報中継装置1では、公開鍵OC2およびOD2を用いて前記と同様に情報を再暗号化してそれぞれの加入者受信端末C3、D3に送信する。これを受信した各受信加入者端末C3、D3では、自身の秘密鍵SC3、SD3を用いて前記再暗号化情報を平文化する。

【0057】このように、本実施例によれば各加入者の公開鍵の情報は暗号化情報中継装置1が集中管理しており、各加入者が管理しているのは共通公開鍵OM1と各自の公開鍵と秘密鍵の組み合わせのみである。したがっ

て、各加入者が加入者共通の秘密鍵を管理する必要がなく、加入者の脱退・新規加入の場合には暗号化情報中継装置1のデータを書き換えるだけでよく、同報暗号通信システムの管理者のみでこれらの脱退・新規加入に迅速に対応できる。したがって、脱退・加入にともなって残存加入者に対して加入者共通の公開鍵および秘密鍵を再度設定しなくてもよい。

【0058】

【実施例2】図5は本発明の実施例2のシステム構成を示すブロック図である。本実施例2のシステム構成は前記実施例1で説明した図2とほぼ同様であるが、暗号化情報に電子署名がなされている点が異なる。

【0059】本実施例において発信加入者端末A3から暗号化情報中継装置1を経由して受信加入者端末B3、C3、D3に送信する場合について以下に説明する。発信加入者端末では、発信加入者端末A3の情報作成部7（図3参照）によって情報を作成する。

【0060】次に、暗号計算部6によって、加入者共通の公開鍵OM1を用いて前記情報を暗号化する。次に発信加入者端末は、暗号計算部6によって前記暗号化情報に対して自身の秘密鍵SA1によって電子署名を行う。

【0061】このようにして生成された暗号化情報と電子署名とを通信インターフェース8を通じて通信回線2上に送信する。このとき、発信加入者端末A3は、同報通信の受信側電子メールのアドレスを指定する。

【0062】電子メールシステム222では、暗号化情報と電子署名とをメールアドレスに従って暗号化情報中継装置1に送信する。暗号化情報中継装置1が通信インターフェース8を通じて前記暗号化情報と電子署名とを受信すると、制御部12の制御により暗号計算部6を通じて加入者共通の秘密鍵SM1を用いて当該暗号化情報を平文化した後、前記電子署名を検証する。この検証は、具体的には鍵格納部11に登録された発信加入者の公開鍵OA2を用いることによって前記電子署名の正当性を確認できる。

【0063】次に、メンバ判断部は、メンバ情報格納部14を参照して、発信者の電子メールアドレスを用いて、送信者が正規の加入者であるか否かを判定する。次に、制御部13は暗号計算部6を制御して、前記情報に対して加入者共通の秘密鍵SM1によって電子署名する。

【0064】次に制御部12は、暗号計算部6を制御して情報を各加入者の公開鍵で暗号化して暗号化情報を生成する。たとえば加入者端末B3に送信する情報であれば公開鍵OB2を用いて暗号化し、加入者端末C3に送信する情報であれば公開鍵OC3を用いて暗号化する。

【0065】次に暗号化情報中継装置1は、前記で再暗号化された情報と電子署名とを通信インターフェース8を通じて電子メールシステム222に送信する。電子メールシステム222では、暗号化情報と電子署名とを各

加入者のメールアドレスに従って各加入者に送信する。

【0066】前記暗号化情報と電子署名とを受信した加入者（たとえば加入者端末B3）は、自身の制御部5を通じて暗号計算部6によって各自の秘密鍵（たとえばSB3）を用いて前記暗号化情報を復号する。

【0067】次に受信側加入者端末B3は、暗号計算部6を通じて加入者共通の公開鍵OM1を用いて前記電子署名を検証する。このように本実施例によれば、電子署名を用いることにより、発信者が自分の身元を保証する手段を実現し、また暗号化情報中継装置1が加入者になりすますことを防止できる。すなわち、受信加入者としては電子署名を検証することにより、発信者が非合法であるか否か、つまり第三者が暗号化情報中継装置1になりすましているか否かを容易に確認することができる。

【0068】

【実施例3】図6は本発明の実施例3のシステム構成を示すブロック図である。本実施例3のシステム構成は前記実施例2で説明した図5とほぼ同様であるが、暗号化を行わずに電子署名のみで平文情報を通信する点が特徴である。

【0069】本実施例において発信加入者端末A3から暗号化情報中継装置1を経由して受信加入者端末B3、C3、D3に送信する場合について以下に説明する。なお、加入者端末の構成および暗号化情報中継装置1の構成については先に説明した図3および図4を用いる。

【0070】発信加入者端末A3では、制御部5の制御情報作成部7によって送信すべき情報を作成する。次に制御部5の制御により暗号計算部6を通じて当該情報に対して発信加入者の秘密鍵SA1を用いて電子署名する。

【0071】発信加入者端末は、前記情報と電子署名とを通信インターフェース8を通じて電子メールシステム222に送信する。電子メールシステム222は、電子メールアドレスにしたがって、前記情報と電子署名とを暗号化情報中継装置1に送信する。

【0072】前記情報と電子署名とを受信した暗号化情報中継装置1では、暗号計算部6を通じて当該電子署名を検証する。そして、メンバ判断部13によってメンバ情報格納部14を参照し、発信者のメールアドレスに基づいて当該発信者が正規の加入者であるか否かを判定する。

【0073】次に制御部12の制御により暗号計算部6を通じて当該情報を加入者共通の秘密鍵SM1を用いて電子署名する。このようにして得られた情報と電子署名と制御部12はを通信インターフェース8を通じて電子メールシステム222に送信する。

【0074】電子メールシステム222を経由して前記情報と電子署名とを受信した加入者端末（たとえばB3）は、自身の暗号計算部6を通じて加入者共通の公開鍵OM1を用いて前記電子署名を検証する。

【0075】このように本実施例によれば、暗号化を行うことなく平文のまま情報を送信する場合にも、電子署名を用いることにより、発信者が自分の身元を保証する手段を実現でき、受信加入者としては電子署名を検証することにより、発信者が非合法であるか否かを容易に確認することができ、不要な情報を読む前に拒絶することができる。

【0076】

【実施例4】図7は、本発明の実施例4における暗号化情報中継装置21を示している。本実施例の暗号化情報中継装置21は、前述の実施例1で説明した暗号化情報中継装置1の構成とほぼ同様であるが、同報方式判断部22が設けられている点が特徴である。

【0077】なお、全体のシステム構成については図2と同様であるので説明の便宜上図2を用いる。前記同報方式判断部22のさらに詳しい構成を示したものが図8である。同図において同報方式判断部22は、発信者情報判断部23、同報方式選択部24および同報方式指示部25で構成されている。発信者情報判断部23は、発信者からの情報がどのようなモードで送信されたかを判断するもので、発信加入者端末から暗号化情報中継装置21に至る情報のモードとしては以下の2通りがある。

(1) 情報と、この情報を発信者の秘密鍵で電子署名したもの

(2) 情報を加入者共通の公開鍵で暗号化した暗号化情報と、情報を発信者の秘密鍵で署名したもの

上記(1)は情報が平文で送信された場合であり、

(2)は情報が暗号で送信された場合である。

【0078】同報方式選択部24は、当該暗号化情報中継装置21より受信加入者端末までの情報のモードを選択する機能を有している。このモードとしては以下の4通りがある。

(3) 情報と、情報を加入者共通の秘密鍵で署名したもの

(4) 情報を各加入者の公開鍵で暗号化した暗号化情報と、情報を加入者共通の秘密鍵で電子署名したもの

(5) 発信者から送信されてきた情報の電子署名の検証結果を情報に添付した検証結果添付情報と、検証結果添付情報を加入者共通の秘密鍵で署名したもの

(6) 発信者から送信されてきた情報の電子署名の検証結果を情報に添付した検証結果添付情報を、各加入者の公開鍵で暗号化したものと、検証結果添付情報を加入者共通の秘密鍵で電子署名したもの

同報方式選択部24は、前記(1)と(3)～(6)との組み合わせ、または前記(2)と(3)～(6)との組み合わせによる合計8通りのモードを選択することが可能である。

【0079】同報方式選択部24による選択に際しては、当該システムの状態に応じて必要とする機密性のレベルを選べば良く、たとえば(1)と(3)の組み合わ

せによれば前述の実施例3に説明した平文情報に電子署名を伴う通信方式となり、最も高い機密性を要求する場合には(2)と(6)との組み合わせとなる。すなわち、(2)と(6)との組み合わせでは、暗号化情報と電子署名とを通信対象とし、暗号化情報中継装置21で検証した電子署名の検証結果をも受信加入者端末に送信されるため、受信者は機密性の保証をより高く受けられることになる。

【0080】以上の各実施例の説明では加入者端末の鍵格納部に加入者の公開鍵と秘密鍵とが登録されている例で説明したが、これらの端末における鍵格納部は固定的なものではなく、たとえば加入者は、ICカード等の記録媒体に共通公開鍵と自身の公開鍵および秘密鍵を登録しておき、これを持参し、必要な場合に近くの汎用的な端末装置のICカードスロットに当該ICカードを装着することにより各実施例で説明したような当該加入者固有の加入者端末を実現するようにしてもよい。

【0081】また以上の各実施例の説明では、暗号通信方式としてPEMを用いたが、他の通信方式であってもよいことは勿論である。また暗号方式としてもRSAに限られない。

【0082】

【発明の効果】本発明によれば、同報暗号通信において、各メンバが管理しなければならない秘密情報を最小限に抑制し、メンバの加入・脱退にも柔軟に対応できる。

【図面の簡単な説明】

【図1】本発明の原理図

【図2】本発明の実施例1におけるシステム構成を示すブロック図

【図3】実施例1において加入者端末装置の内部構成を示すブロック図

【図4】実施例1における暗号化情報中継装置の内部構成を示すブロック図

【図5】本発明の実施例2のシステム構成を示すブロック図

【図6】本発明の実施例3のシステム構成を示すブロック図

【図7】本発明の実施例4における暗号化情報中継装置21の構成を示すブロック図

【図8】実施例4における同報方式判断部の構成を示すブロック図

【図9】共通鍵方式を説明するためのシステム構成図

【図10】個別鍵方式を説明するためのシステム構成図

【符号の説明】

100・・・情報

A3, B3, C3・・・加入者端末

1・・・暗号化情報中継装置

2・・・通信回線

3a・・・鍵格納部

13

14

- 5・・・制御部
- 6・・・暗号計算部
- 7・・・情報作成部
- 8・・・通信インターフェース
- 11・・・鍵格納部
- 13・・・メンバ判断部
- 14・・・メンバ情報格納部
- 21・・・暗号化情報中継装置
- 22・・・同報方式判断部

* 201・・・通信回線

202a, 202b, 202c, 202d・・・加入者
(加入者端末)

203・・・暗号計算部

204・・・共通秘密鍵

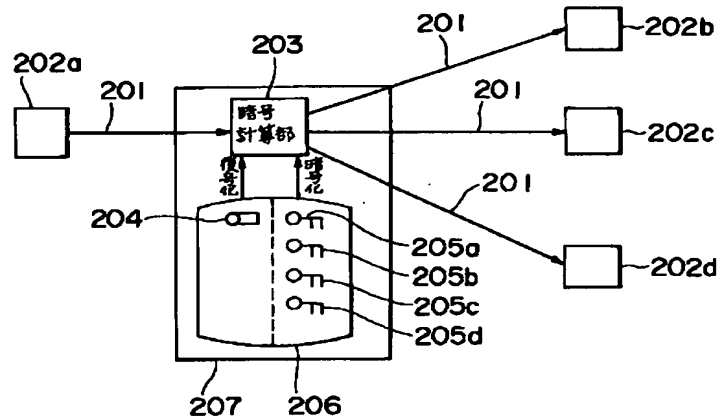
205a, 205b, 205c, 205d・・・個別公開
鍵

206・・・鍵格納部

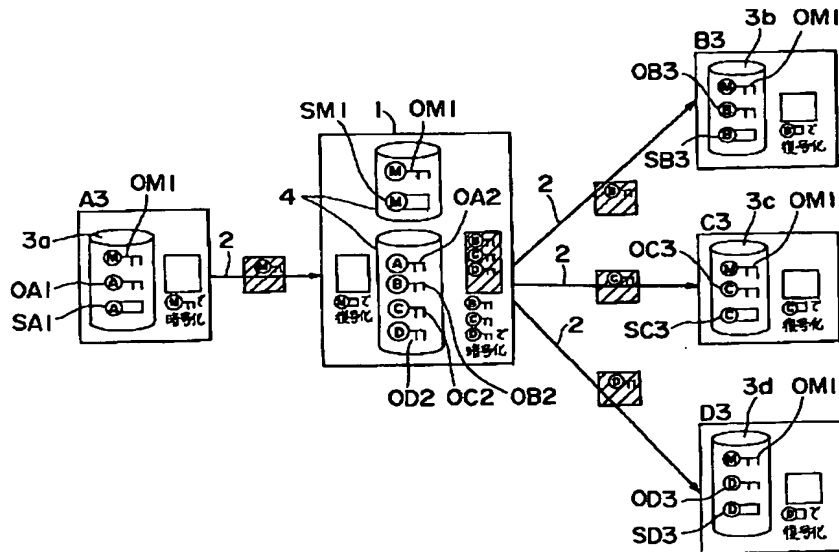
* 222・・・電子メールシステム

10

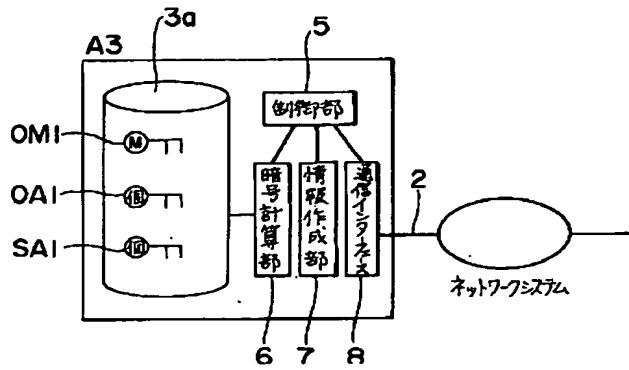
【図1】



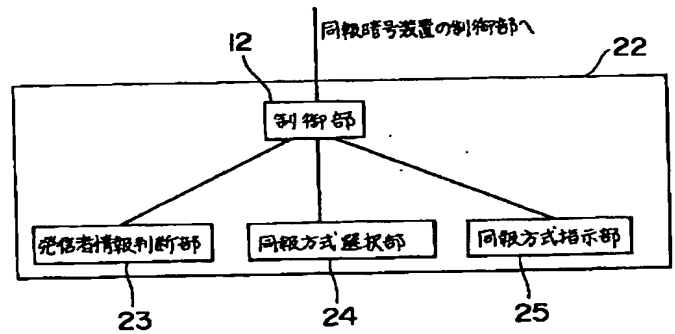
【図2】



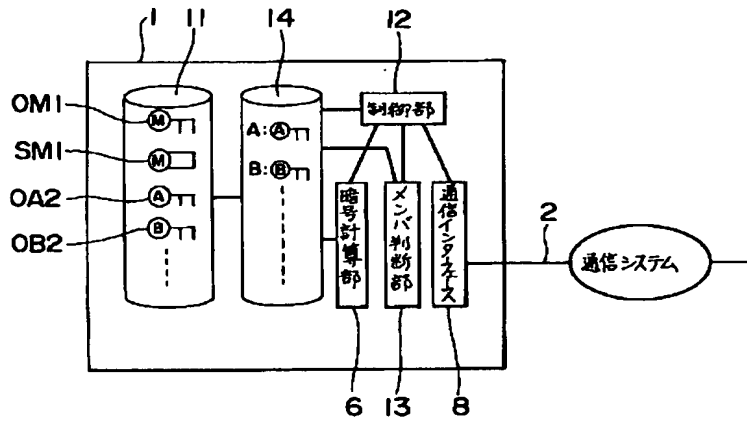
【図 3】



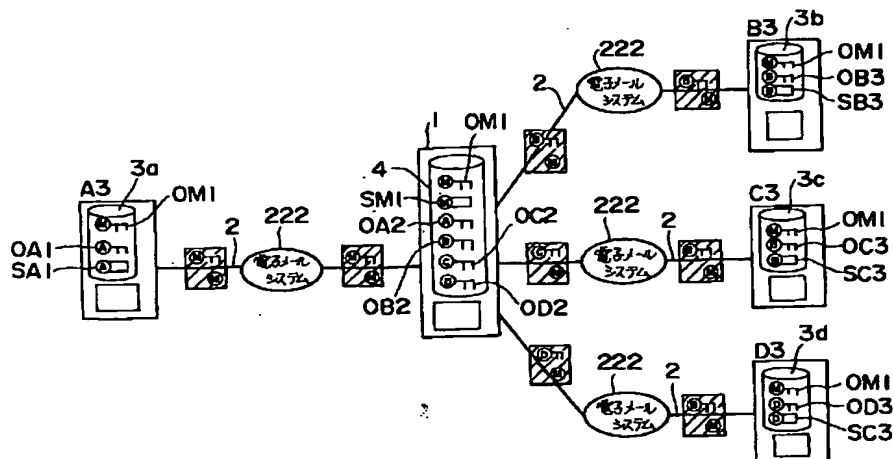
【図 8】



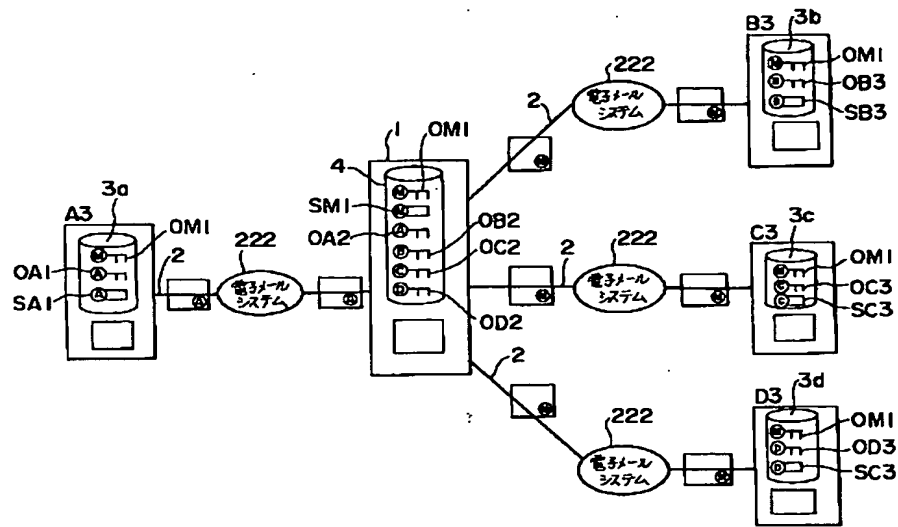
【図 4】



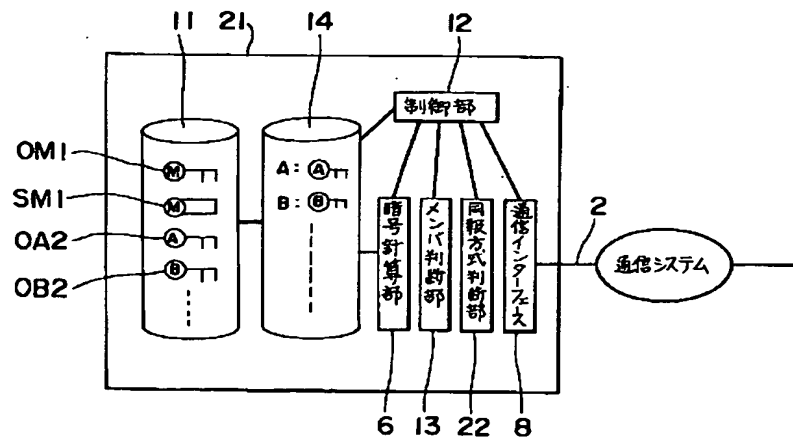
【図 5】



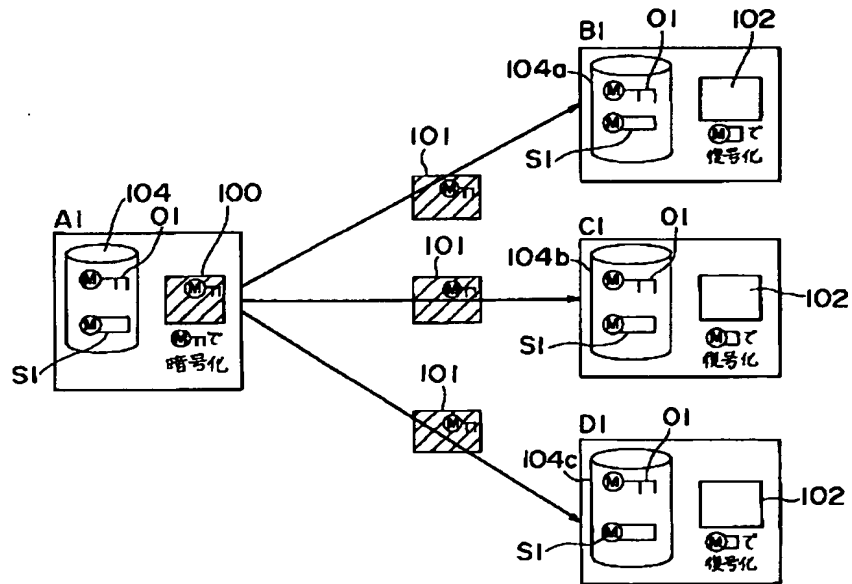
【図 6】



【図 7】



【図 9】



【図 10】

